ALB:RAS
F. #2020R00501

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE 11 PRO MAX, WITH SERIAL NUMBER F2LZF59XN711 AND IMEI 353920100403155, CURRENTLY LOCATED WITHIN THE EASTERN DISTRICT OF NEW YORK	**APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE** Case No. 21-353-M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, DAVID NIGRO, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with HSI and have been for approximately four years. During that time, I have been involved in the investigation of cases involving financial crimes and frauds, including wire fraud, and I have participated in the execution of numerous warrants, including warrants to search electronic devices like the one sought herein.

3. I have been personally involved in the investigation of this matter, and I base this affidavit on that participation, my conversations with other law enforcement agents and other individuals, my examination of reports and records, as well as my training and experience. Where the contents of conversations of others are reported herein, they are reported in substance and in part.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone 11 Pro Max, with serial number F2LZF59XN711, and IMEI 353920100403155, hereinafter the "Device." The Device is currently in the possession of a law enforcement agent within the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On March 13, 2021, the Honorable Cheryl L. Pollak, United States Magistrate Judge, signed a Complaint charging Sushmita Tabassum with wire fraud in violation of Title 18, United States Code, Section 1343. (See 21-314-M.) That same day Judge Pollak signed a warrant for Tabassum's arrest. The Complaint and arrest warrant were issued based in part on the facts set forth below.

Criminal Conduct

8. In or about July 2015, Tabassum began working at John Doe Company in Queens, New York (the "Company"). In or about July 2019, she became the acting CEO and manager of the Company.

9. The Company is a licensed money transfer business based in New York and is a branch of a company in Bangladesh (the "Bangledesh Company"). The Company receives cash from customers who wish to transmit funds to Bangladesh, and the Bangladesh Company distributes the money to the intended recipient in Bangladesh. The cash provided by customers in New York is deposited at various intervals into the Company's account at a bank (the "Bank") and transferred to the Bangladesh Company's account at the Bank. Prior to being deposited into the account at the Bank, the money is held in a safe at the Company's store in Queens.

10. Agents of the Company reported that from late July 2019 until early February 2020, only Tabassum and one other employee ("Employee-1") worked on-site at the Company's Queens location, and Tabassum was solely responsible for bookkeeping and bank deposits into the Company's Bank account. As part of her responsibilities, Tabassum sent a daily email from the Queens office to agents of the Bangladesh Company in Bangladesh reporting the money the Company had received that day and directing agents at the Bangladesh Company as to where the money needed to be sent in Bangladesh.

11. In or about February 2020, in the normal course of business, the Company assigned a new manager ("Employee-2") to the location in Queens. Upon beginning his employment, Employee-2 conducted an audit of the business and determined that approximately $600,000 was not accounted for, meaning it had neither been deposited into the Company account at the Bank, nor was it in the safe at the store.

12. Employee-2 reported that he asked Tabassum about the missing funds, after which Tabassum presented Employee-2 with a book of receipts reflecting deposits into the Company's Bank account. Among those Bank deposit receipts were purported receipts for three deposits totaling approximately $509,820, which would have accounted for the majority of the missing funds. Specifically, Tabassum presented purported Bank receipts for: (i) a deposit on January 14, 2020 of $197,010; (ii) a deposit on January 15, 2020 of $148,203; and (iii) a deposit on January 21, 2020 of $164,607 (the "Three Deposits" or the "Three Deposit Receipts").

13. On February 18, 2020, Tabassum wrote and signed a letter to the Bank stating that she had deposited the Three Deposits at the Bank on the specified dates and asking the Bank to "arrange to credit" the account for the three deposits.

14. On February 21, 2020, the Bank wrote a letter stating that the Company did not make those deposits on the dates indicated and noting that that information had been communicated to Tabassum at a meeting previously held at the Bank. Accordingly, the Bank declined the request as invalid and closed the file on Tabassum's claim. Subpoenaed records from the Bank further show that no deposits were made into the Company's account on those dates.

15. Law enforcement has compared the Three Deposit Receipts with verified Bank deposit receipts and noted several differences that suggest the Three Deposit Receipts are fraudulent. The Company also independently hired a forensic document examiner who also concluded that the Three Deposit Receipts were fake and had not been generated by the Bank. Among other things, the paper on which the Three Deposit Receipts are printed is a different type of paper than that of the verified receipts, the font used is noticeably different and the Three

Deposit Receipts all contain identical fading of certain text, which suggests they were all created using the same scanned image as a template.

Departure from and Return to the United States

16. On or about June 2020, Tabassum boarded a flight departing from John F. Kennedy International Airport ("JFK") destined for Doha International Airport in Qatar. To my knowledge, Tabassum did not return to the United States until March 13, 2021.

17. On March 13, 2021, Tabassum entered the United States through JFK at approximately 6:25pm on a flight originating in Turkey.

The Device

18. When Tabassum arrived at JFK, she was in possession of the Device. I placed the Device in airplane mode and manually searched it pursuant to the border search authority.

19. Upon a preliminary review of the Device, I found numerous photographs relating to financial transactions and accounts, as well as images of apparently expensive items.

20. For example, the Device contains the following:

a. Multiple photographs of jewelry taken on or about August 6, 2019;

b. A photograph taken on or about August 8, 2019 of a handwritten note with an unknown person's name, together with an account number, a password, a routing number, credit card details and a pin number;

c. A photograph taken on or about September 27, 2019 of Tabassum wearing jewelry that appears to have multiple diamonds;

d. Multiple photographs taken on or about October 21, 2019 of jewelry still in its packaging and of multiple bags and purses;

e. A photograph, taken on or about October 22, 2019 of a Michael Kors bag still in its packaging, together with a screenshot of a Michael Kors purse from the Michael Kors' website reflecting a retail price of $289.00;

f. A photograph taken on or about April 15, 2020 of a Mastercard bearing Tabassum's name, a Platinum card bearing Tabassum's name and a Quicksilver CapitalOne card bearing Tabassum's name;

g. A photograph take on or about June 29, 2020 of a receipt from Standard Charter Bank for a cash deposit of 10,000 (the currency type is not listed); and

h. A photograph taken on or about July 16, 2020 of a handwritten note reflecting CapitalOne banking information, including a routing number.

21. The Device also contains photographs taken on or about February 27, 2020, of the Three Deposit Receipts.

22. Based on my training and experience, I know that individuals who engage in the embezzlement or theft of large sums of money will often maintain bank account and other financial information on electronic devices. Such individuals will often maintain multiple bank accounts and bank cards to maintain the stolen funds.

23. Further, such individuals will often make expensive purchases and may take photographs of those purchases. Such purchases are often made online and evidence of such purchases is frequently maintained on electronic devices through internet browser history, photographs, communications and otherwise.

24. The Device is currently in the lawful possession of HSI. It came into HSI's possession after it was seized pursuant to the border search authority and incident to Tabassum's

arrest as described above. Therefore, while HSI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

25. The Device is currently in the possession of a law enforcement agent within the Eastern District of New York and has previously been stored at HSI's offices. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and

storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This

removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on

devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

i. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

k. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

l. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

David Nigro
Special Agent
United States Department of Homeland Security, Homeland Security Investigations

Subscribed and sworn to before me by telephone on March 23, 2021

[redacted]

HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is an Apple iPhone 11 Pro Max, with serial number F2LZF59XN711, and IMEI 353920100403155, hereinafter the "Device." The Device is currently in the possession of a law enforcement agent within the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 1343 (wire fraud), 1344 (bank fraud) and 1956 (money laundering) and involve Sushmita Tabassum since July 1, 2019, including:

   a. Evidence of and records or information relating to unexplained funds or expensive purchases, such as photographs of apparently expensive items, records and information related to such purchases, photographs of cash, or records and information relating to money deposits or transactions;

   b. Communications relating any transfer of funds, unexplained funds or expensive purchases or a scheme to defraud Tabassum's employer or the Bank;

   c. any information recording Tabassum's schedule or travel from July 1, 2019 to the present;

   d. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.